



Atty. Docket No.: 096790.P355

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re the application of: )  
)  
Satoshi Shigematsu, et al )  
)  
Serial No.: 09/853,770 )  
)  
Assigned Filing Date: May 11, 2001 )  
)  
For: AUTHENTICATION TOKEN AND AUTHENTICATION SYSTEM )

PRIORITY DOCUMENT SUBMITTAL

Hon. Commissioner of  
Patents and Trademarks  
Washington, D.C. 20231

Dear Sir:

Submitted herewith is a document upon which Applicant respectfully requests a convention priority for the above-captioned application, namely Japanese Patent Application No. 2001-004998 filed January 12, 2001, Japanese Patent Application No. 2001-005002, Japanese Patent Application No. 2001-005033, Japanese Patent Application No 2001-103058, Japanese Patent Application No. 2001-103066, and Japanese Patent Application No. 2001-104331.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN

Dated: 7/27/01

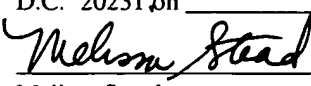
By: 

Eric S. Hyman, Reg. No. 30,139

**CERTIFICATE OF MAILING**

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to:

Assistant Commissioner for Patents, Washington,  
D.C. 20231 on 7-23-01



Melissa Stead

7-23-01

Date

12400 Wilshire Boulevard  
Seventh Floor  
Los Angeles, California 90025  
(310) 207-3800



P14683-A

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2001年 1月12日

出 願 番 号

Application Number:

特願2001-004998

出 願 人

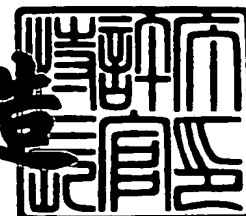
Applicant(s):

日本電信電話株式会社

2001年 6月13日

特 許 庁 長 官  
Commissioner,  
Japan Patent Office

及 川 耕 造



出証番号 出証特2001-3055433

【書類名】 特許願

【整理番号】 NTTH126777

【提出日】 平成13年 1月12日

【あて先】 特許庁長官殿

【国際特許分類】 G06K 9/00

【発明者】

【住所又は居所】 東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内

【氏名】 重松 智志

【発明者】

【住所又は居所】 東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内

【氏名】 海野 秀之

【発明者】

【住所又は居所】 東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内

【氏名】 久良木 億

【特許出願人】

【識別番号】 000004226

【氏名又は名称】 日本電信電話株式会社

【代理人】

【識別番号】 100064621

【弁理士】

【氏名又は名称】 山川 政樹

【電話番号】 03-3580-0961

【手数料の表示】

【予納台帳番号】 006194

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9701512

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 認証システムおよび方法、記録媒体、プログラム

【特許請求の範囲】

【請求項 1】 ユーザが所定のサービスを提供するサービス提供装置を利用する場合に必要なユーザ認証を当該ユーザの生体情報を用いて行う認証システムであって、

通常時はユーザにより所持されるとともに、ユーザが前記サービス提供装置を利用する場合はそのサービス提供装置へ接続されて前記ユーザの生体情報に基づきユーザ認証を行う認証トークンを備え、

この認証トークンは、ユーザから検出した生体情報をもとにユーザ本人であることを照合する本人照合装置と、当該認証トークンのパスワードと当該認証トークンを識別するためのトークン識別情報とを記憶する記憶回路と、前記本人照合装置での照合結果が照合成功を示す場合に前記記憶回路のパスワードおよびトークン識別情報とを通信データとして前記サービス提供装置へ送信する第 1 の通信装置とを有し、

前記サービス提供装置は、前記認証トークンからの通信データを受信する第 2 の通信装置と、前記認証トークンのトークン識別情報とパスワードとを関連付けて予め記憶する第 1 のデータベースと、前記通信データに含まれるパスワードと前記トークン識別情報をキーとして前記第 1 のデータベースから検索したパスワードとを照合する照合回路と、この照合回路での照合結果に基づき前記ユーザに対してサービスを提供する処理装置とを有することを特徴とする認証システム。

【請求項 2】 請求項 1 記載の認証システムにおいて、

通信ネットワークを介して前記サービス提供装置へ接続され、前記データベースに対して前記トークン識別情報とパスワードとを関連付けて登録する登録装置をさらに備えることを特徴とする認証システム。

【請求項 3】 請求項 1 または 2 記載の認証システムにおいて、

前記サービス提供装置は、新規パスワードを発生させて前記第 2 の通信装置を介して前記認証トークンへ送信するとともに、前記第 1 のデータベースに記憶されている前記パスワードを更新するパスワード発生回路を有し、

前記認証トークンの第 1 の通信装置は、前記サービス提供装置から受信した新規パスワードにより記憶回路で記憶しているパスワードを更新することを特徴とする認証システム。

【請求項 4】 請求項 1 ～ 3 記載の認証システムにおいて、

前記サービス提供装置は、当該サービス提供装置を識別するための装置識別情報を記憶する記憶回路を有し、前記第 2 の通信装置は、前記認証トークンの接続に応じて前記記憶回路から装置識別情報を読み出して前記認証トークンへ送信し、

前記認証トークンは、前記サービス提供装置を識別するための装置識別情報とパスワードとを関連付けて記憶する第 2 のデータベースを有し、前記第 1 の通信装置は、前記サービス提供装置へ送信するパスワードとして、前記サービス提供装置から受信した装置識別情報をキーとして前記第 2 のデータベースから検索したパスワードを用いることを特徴とする認証システム。

【請求項 5】 ユーザが所定のサービスを提供するサービス提供装置を利用する場合に必要なユーザ認証を、当該ユーザの生体情報を用いてユーザ認証を行う認証トークンと前記サービス提供装置との間で行う認証方法であって、

前記認証トークンは、当該認証トークンのパスワードと当該認証トークンを識別するためのトークン識別情報とを予め記憶し、ユーザから検出した生体情報をもとにユーザ本人であることを照合し、その照合結果が照合成功を示す場合に前記パスワードおよびトークン識別情報を通信データとして前記サービス提供装置へ送信し、

前記サービス提供装置は、前記認証トークンのトークン識別情報とパスワードとを第 1 のデータベースで関連付けて予め記憶し、前記認証トークンから受信した通信データに含まれるパスワードと前記トークン識別情報をキーとして前記第 1 のデータベースから検索したパスワードとを照合し、その照合結果に基づき前記ユーザに対してサービスを提供することを特徴とする認証方法。

【請求項 6】 請求項 5 記載の認証方法において、

通信ネットワークを介して前記サービス提供装置へ接続された登録装置から、前記第 1 のデータベースに対して前記トークン識別情報とパスワードとを関連付

けて登録することを特徴とする認証方法。

【請求項 7】 請求項 5 または 6 記載の認証方法において、

前記サービス提供装置は、新規パスワードをパスワード発生回路で発生させ、前記第 2 の通信装置を介して前記認証トークンへ送信するとともに、前記第 1 のデータベースに記憶されている前記パスワードを更新し、

前記認証トークンは、前記サービス提供装置から受信した新規パスワードにより予め記憶しているパスワードを更新することを特徴とする認証方法。

【請求項 8】 請求項 5 ～ 7 記載の認証方法において、

前記サービス提供装置は、当該サービス提供装置を識別するための装置識別情報を予め記憶し、前記認証トークンの接続に応じて前記装置識別情報を前記認証トークンへ送信し、

前記認証トークンは、前記サービス提供装置を識別するための装置識別情報とパスワードとを関連付けて第 2 のデータベースで予め記憶し、前記サービス提供装置へ送信するパスワードとして、前記サービス提供装置から受信した装置識別情報をキーとして前記第 2 のデータベースから検索したパスワードを用いることを特徴とする認証方法。

【請求項 9】 ユーザが所定のサービスを提供するサービス提供装置を利用する場合に必要なユーザ認証を、当該ユーザの生体情報を用いてユーザ認証を行う認証トークンと前記サービス提供機器との間で行う認証手順をコンピュータで実行させるためのプログラムが記載された記録媒体であって、

前記サービス提供装置で、前記認証トークンのトークン識別情報とパスワードとを第 1 のデータベースで関連付けて予め記憶するステップと、前記認証トークンでのユーザから検出した生体情報をもとにしたユーザ本人の照合後、その照合結果が照合成功を示す場合に当該認証トークンから送信された当該認証トークンのパスワードおよび当該認証トークンを識別するためのトークン識別情報を含む通信データを受信するステップと、その通信データに含まれる前記パスワードと前記トークン識別情報をキーとして前記第 1 のデータベースから検索したパスワードとを照合するステップと、その照合結果に基づき前記ユーザに対してサービスを提供するステップとを実行させるためのプログラムが記載された記録媒体。

【請求項 1 0】 請求項 9 記載の記録媒体において、

前記サービス提供装置で、通信ネットワークを介して前記サービス提供装置へ接続された登録装置から、前記第 1 のデータベースに対して前記トークン識別情報とパスワードとを関連付けて登録するステップを実行させるためのプログラムがさらに記載された記録媒体。

【請求項 1 1】 請求項 9 または 1 0 記載の記録媒体において、

前記サービス提供装置で、新規パスワードをパスワード発生回路で発生させるステップと、前記新規パスワードを前記第 2 の通信装置を介して前記認証トークンへ送信することにより当該認証トークンで予め記憶しているパスワードを更新するステップと、前記新規パスワードにより前記第 1 のデータベースに記憶されている前記パスワードを更新するステップとを実行させるためのプログラムがさらに記載された記録媒体。

【請求項 1 2】 請求項 9 ～ 1 1 記載の記録媒体において、

前記サービス提供装置で、当該サービス提供装置を識別するための装置識別情報を予め記憶するステップと、前記認証トークンの接続に応じて前記装置識別情報を前記認証トークンへ送信することにより、前記認証トークンでの前記サービス提供装置の識別に用いる装置識別情報とパスワードとを関連付けて当該認証トークンの第 2 のデータベースへ記憶させ、前記サービス提供装置へ送信するパスワードとして、前記サービス提供装置から受信した装置識別情報をキーとして前記第 2 のデータベースからパスワードを検索させるステップとを実行させるためのプログラムがさらに記載された記録媒体。

【請求項 1 3】 ユーザが所定のサービスを提供するサービス提供装置を利用する場合に必要なユーザ認証を、当該ユーザの生体情報を用いてユーザ認証を行う認証トークンと前記サービス提供機器との間で行う認証手順をコンピュータで実行させるためのプログラムであって、

前記サービス提供装置で、前記認証トークンのトークン識別情報とパスワードとを第 1 のデータベースで関連付けて予め記憶するステップと、前記認証トークンでのユーザから検出した生体情報をもとにしたユーザ本人の照合後、その照合結果が照合成功を示す場合に当該認証トークンから送信された当該認証トークン



のパスワードおよび当該認証トークンを識別するためのトークン識別情報を含む通信データを受信するステップと、その通信データに含まれる前記パスワードと前記トークン識別情報をキーとして前記第 1 のデータベースから検索したパスワードとを照合するステップと、その照合結果に基づき前記ユーザに対してサービスを提供するステップとを実行させるためのプログラム。

【請求項 1 4】 請求項 1 3 記載のプログラムにおいて、

前記サービス提供装置で、通信ネットワークを介して前記サービス提供装置へ接続された登録装置から、前記第 1 のデータベースに対して前記トークン識別情報とパスワードとを関連付けて登録するステップを実行させるためのプログラム

。

【請求項 1 5】 請求項 1 3 または 1 4 記載のプログラムにおいて、

前記サービス提供装置で、新規パスワードをパスワード発生回路で発生させるステップと、前記新規パスワードを前記第 2 の通信装置を介して前記認証トークンへ送信することにより当該認証トークンで予め記憶しているパスワードを更新するステップと、前記新規パスワードにより前記第 1 のデータベースに記憶されている前記パスワードを更新するステップとを実行させるためのプログラム。

【請求項 1 6】 請求項 1 3 ～ 1 5 記載のプログラムにおいて、

前記サービス提供装置で、当該サービス提供装置を識別するための装置識別情報を予め記憶するステップと、前記認証トークンの接続に応じて前記装置識別情報を前記認証トークンへ送信することにより、前記認証トークンでの前記サービス提供装置の識別に用いる装置識別情報とパスワードとを関連付けて当該認証トークンの第 2 のデータベースへ記憶させ、前記サービス提供装置へ送信するパスワードとして、前記サービス提供装置から受信した装置識別情報をキーとして前記第 2 のデータベースからパスワードを検索させるステップとを実行させるためのプログラム。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、認証システムおよび方法、記録媒体、プログラムに関し、特に認証

トークンで人間の生体情報を用いてユーザ本人であることを認証する認証システムおよび方法、記録媒体、プログラムに関するものである。

#### 【 0 0 0 2 】

##### 【従来の技術】

高度情報化社会では、情報処理との親和性を持って厳密にユーザ本人を認証したいという要求が高い。特に、予め承認したユーザだけに入室を許可する入室管理システムや個人情報などの重要な情報を扱うような情報管理システム、あるいは電子決済を行う決済システムなどでは、上記のような要求が極めて高い。

このような要求に対し、半導体装置の製造技術や情報処理技術をベースとして、電子的に検出した固有の生体情報に基づきユーザ本人を認証する認証トークンを用いた認証システムの研究が盛んに行われている。

#### 【 0 0 0 3 】

このような認証システムとして、例えば図 6 に示すような構成が考えられる。

この認証システムでは、ユーザの指紋などの生体情報を用いてユーザ本人の認証を行う認証トークン 8 と、この認証トークン 8 からの本人照合結果に基づきそのユーザへサービスを提供するサービス提供装置 9 とから構成されている。

このシステムでは、認証トークン 8 内の本人照合装置 8 1 で生体情報に基づき本人照合が行われ、その本人照合結果 8 1 A が通信回路 8 2 を介してサービス提供装置 9 に送信される。サービス提供装置 9 はこの本人照合結果を通信回路 9 1 を介し受信し、その本人照合結果 9 1 A が照合成功を示す場合に処理装置 9 2 で処理を行うことによりユーザへサービスの提供を行うものとなっている。

#### 【 0 0 0 4 】

##### 【発明が解決しようとする課題】

しかしながら、このような認証システムでは、認証トークン 8 から送信される照合結果をもとにサービス提供装置 9 でサービス提供の可否を決定しているため、例えば、常に照合成功の結果を出力する偽造認証トークンを用いることで、不正にサービスを利用することが可能になってしまうという問題点があった。また、任意のユーザに対してサービス提供の可否を制限することも不可能であり、任意のサービスに対して利用ユーザを制限することも不可能であった。

本発明はこのような課題を解決するためのものであり、サービスの不正利用を防止できるとともに、利用ユーザを特定できる認証システムおよび方法、記録媒体、プログラムを提供することを目的としている。

## 【 0 0 0 5 】

## 【課題を解決するための手段】

このような目的を達成するために、本発明にかかる認証システムは、ユーザが所定のサービスを提供するサービス提供装置を利用する場合に必要なユーザ認証を当該ユーザの生体情報を用いて行う認証システムであって、通常時はユーザにより所持されるとともに、ユーザがサービス提供装置を利用する場合はそのサービス提供装置へ接続されてユーザの生体情報に基づきユーザ認証を行う認証トークンを備え、この認証トークンに、ユーザから検出した生体情報をもとにユーザ本人であることを照合する本人照合装置と、当該認証トークンのパスワードと当該認証トークンを識別するためのトークン識別情報とを記憶する記憶回路と、本人照合装置での照合結果が照合成功を示す場合に記憶回路のパスワードおよびトークン識別情報とを通信データとしてサービス提供装置へ送信する第1の通信装置とを設け、サービス提供装置に、認証トークンからの通信データを受信する第2の通信装置と、認証トークンのトークン識別情報とパスワードとを関連付けて予め記憶する第1のデータベースと、通信データに含まれるパスワードとトークン識別情報をキーとして第1のデータベースから検索したパスワードとを照合する照合回路と、この照合回路での照合結果に基づきユーザに対してサービスを提供する処理装置とを設けたものである。

## 【 0 0 0 6 】

サービス提供装置に対する認証トークンの登録については、通信ネットワークを介してサービス提供装置へ接続される登録装置を設け、データベースに対してトークン識別情報とパスワードとを関連付けて登録するようにしてもよい。

認証トークンで管理するパスワードについては、サービス提供装置にパスワード発生回路を設け、新規パスワードを発生させて第2の通信装置を介して認証トークンへ送信するとともに、第1のデータベースに記憶されているパスワードを更新するものとし、認証トークンの第1の通信装置で、サービス提供装置から受

信した新規パスワードにより記憶回路で記憶しているパスワードを更新するようにしてもよい。

## 【 0 0 0 7 】

認証トークンのパスワードを各サービス提供装置ごとに使い分けるために、サービス提供装置に、当該サービス提供装置を識別するための装置識別情報を記憶する記憶回路を設け、第2の通信装置で、認証トークンの接続に応じて記憶回路から装置識別情報を読み出して認証トークンへ送信し、認証トークンに、サービス提供装置を識別するための装置識別情報とパスワードとを関連付けて記憶する第2のデータベースを設け、第1の通信装置で、サービス提供装置へ送信するパスワードとして、サービス提供装置から受信した装置識別情報をキーとして第2のデータベースから検索したパスワードを用いるようにしてもよい。

## 【 0 0 0 8 】

また、本発明にかかる認証方法は、ユーザが所定のサービスを提供するサービス提供装置を利用する場合に必要なユーザ認証を、当該ユーザの生体情報を用いてユーザ認証を行う認証トークンとサービス提供機器との間で行う認証方法であって、認証トークンで、当該認証トークンのパスワードと当該認証トークンを識別するためのトークン識別情報とを予め記憶し、ユーザから検出した生体情報をもとにユーザ本人であることを照合し、その照合結果が照合成功を示す場合にパスワードおよびトークン識別情報を通信データとしてサービス提供装置へ送信し、サービス提供装置で、認証トークンのトークン識別情報とパスワードとを第1のデータベースで関連付けて予め記憶し、認証トークンから受信した通信データに含まれるパスワードとトークン識別情報をキーとして第1のデータベースから検索したパスワードとを照合し、その照合結果に基づきユーザに対してサービスを提供するようにしたものである。

## 【 0 0 0 9 】

サービス提供装置に対する認証トークンの登録については、通信ネットワークを介してサービス提供装置へ接続された登録装置から、第1のデータベースに対してトークン識別情報とパスワードとを関連付けて登録するようにしてもよい。

認証トークンで管理するパスワードについては、サービス提供装置で、新規パ

スワードをパスワード発生回路で発生させ、第2の通信装置を介して認証トークンへ送信するとともに、第1のデータベースに記憶されているパスワードを更新し、認証トークンで、サービス提供装置から受信した新規パスワードにより予め記憶しているパスワードを更新するようにしてもよい。

## 【0010】

認証トークンのパスワードを各サービス提供装置ごとに使い分けるために、サービス提供装置で、当該サービス提供装置を識別するための装置識別情報を予め記憶し、認証トークンの接続に応じて装置識別情報を認証トークンへ送信し、認証トークンで、サービス提供装置を識別するための装置識別情報とパスワードとを関連付けて第2のデータベースで予め記憶し、サービス提供装置へ送信するパスワードとして、サービス提供装置から受信した装置識別情報をキーとして第2のデータベースから検索したパスワードを用いるようにしてもよい。

## 【0011】

また、本発明にかかる記録媒体は、ユーザが所定のサービスを提供するサービス提供装置を利用する場合に必要なユーザ認証を、当該ユーザの生体情報を用いてユーザ認証を行う認証トークンと前記サービス提供機器との間で行う認証手順をコンピュータで実行させるためのプログラムが記録された記録媒体であって、サービス提供装置で、認証トークンのトークン識別情報とパスワードとを第1のデータベースで関連付けて予め記憶するステップと、認証トークンでのユーザから検出した生体情報をもとにしたユーザ本人の照合後、その照合結果が照合成功を示す場合に当該認証トークンから送信された当該認証トークンのパスワードおよび当該認証トークンを識別するためのトークン識別情報を含む通信データを受信するステップと、その通信データに含まれるパスワードとトークン識別情報をキーとして第1のデータベースから検索したパスワードとを照合するステップと、その照合結果に基づきユーザに対してサービスを提供するステップとを実行させるためのプログラムが記載された記録媒体である。

## 【0012】

サービス提供装置に対する認証トークンの登録については、サービス提供装置で、通信ネットワークを介してサービス提供装置へ接続された登録装置から、第

1のデータベースに対してトークン識別情報とパスワードとを関連付けて登録するステップをコンピュータで実行させるためのプログラムを記録媒体に記載してもよい。

認証トークンで管理するパスワードについては、サービス提供装置で、新規パスワードをパスワード発生回路で発生させるステップと、新規パスワードを第2の通信装置を介して認証トークンへ送信することにより当該認証トークンで予め記憶しているパスワードを更新するステップと、新規パスワードにより第1のデータベースに記憶されているパスワードを更新するステップとをコンピュータで実行させるためのプログラムを記録媒体に記載してもよい。

#### 【0013】

認証トークンのパスワードを各サービス提供装置ごとに使い分けるために、サービス提供装置で、当該サービス提供装置を識別するための装置識別情報を予め記憶するステップと、認証トークンの接続に応じて装置識別情報を認証トークンへ送信することにより、認証トークンでのサービス提供装置の識別に用いる装置識別情報とパスワードとを関連付けて当該認証トークンの第2のデータベースへ記憶させ、サービス提供装置へ送信するパスワードとして、サービス提供装置から受信した装置識別情報をキーとして第2のデータベースからパスワードを検索させるステップとをコンピュータで実行させるためのプログラムを記録媒体に記載してもよい。

#### 【0014】

また、本発明にかかるプログラムは、ユーザが所定のサービスを提供するサービス提供装置を利用する場合に必要なユーザ認証を、当該ユーザの生体情報を用いてユーザ認証を行う認証トークンと前記サービス提供機器との間で行う認証手順をコンピュータで実行させるためのプログラムであって、サービス提供装置で、認証トークンのトークン識別情報とパスワードとを第1のデータベースで関連付けて予め記憶するステップと、認証トークンでのユーザから検出した生体情報をもとにしたユーザ本人の照合後、その照合結果が照合成功を示す場合に当該認証トークンから送信された当該認証トークンのパスワードおよび当該認証トークンを識別するためのトークン識別情報を含む通信データを受信するステップと、

その通信データに含まれるパスワードとトークン識別情報をキーとして第1のデータベースから検索したパスワードとを照合するステップと、その照合結果に基づきユーザに対してサービスを提供するステップとを実行させるためのプログラムである。

## 【0015】

サービス提供装置に対する認証トークンの登録については、サービス提供装置で、通信ネットワークを介してサービス提供装置へ接続された登録装置から、第1のデータベースに対してトークン識別情報とパスワードとを関連付けて登録するステップをプログラムでさらに実行させるようにしてもよい

認証トークンで管理するパスワードについては、サービス提供装置で、新規パスワードをパスワード発生回路で発生させるステップと、新規パスワードを第2の通信装置を介して認証トークンへ送信することにより当該認証トークンで予め記憶しているパスワードを更新するステップと、新規パスワードにより第1のデータベースに記憶されているパスワードを更新するステップとをプログラムでさらに実行させるようにしてもよい

## 【0016】

認証トークンのパスワードを各サービス提供装置ごとに使い分けるために、サービス提供装置で、当該サービス提供装置を識別するための装置識別情報を予め記憶するステップと、認証トークンの接続に応じて装置識別情報を認証トークンへ送信することにより、認証トークンでのサービス提供装置の識別に用いる装置識別情報とパスワードとを関連付けて当該認証トークンの第2のデータベースへ記憶させ、サービス提供装置へ送信するパスワードとして、サービス提供装置から受信した装置識別情報をキーとして第2のデータベースからパスワードを検索させるステップとをプログラムでさらに実行させるようにしてもよい。

## 【0017】

## 【発明の実施の形態】

次に、本発明の実施の形態について図面を参照して説明する。

図1は本発明の一実施の形態にかかる認証システムのブロック図である。この認証システムは、ユーザにサービスを提供するサービス提供装置2と、ユーザに

所持されるとともにサービス提供時にサービス提供装置 2 に接続されてユーザ本人の認証を行う認証トークン 1 から構成される。なお、本発明において、トークンとは、ユーザが所持し持ち運び可能な小型軽量の装置を指し、認証トークンとは、ユーザ本人の認証を行う機能を持つトークンをいう。以下では、生体情報として指紋を用いる場合を例として説明するが、生体情報としては、このほか声紋、虹彩、筆跡、手のひら形状（指の関節長）、静脈パターン、顔面配置パターンなどを用いることも可能である。

## 【 0 0 1 8 】

認証トークン 1 には、ユーザの生体情報をもとに本人であるか照合を行う本人照合装置 1 1、この認証トークン 1 を識別するためのトークン ID（トークン識別情報）1 2 B などの情報やパスワード 1 2 A を記憶する記憶回路 1 2、本人照合装置 1 1 での本人照合結果 1 1 A が照合成功を示す場合にのみ記憶回路 1 2 に記憶されているトークン ID 1 2 B やパスワード 1 2 A を通信データ 1 A としてトークン外に送信する通信装置（第 1 の通信装置）1 3 が設けられている。なお、本人照合装置 1 1 には、指紋画像を取得するセンサ、予めユーザの指紋画像またはその特徴を示す登録データを記憶する記憶部、記憶部の登録データを用いてセンサからの指紋画像を照合し照合結果を出力する照合部が設けられている。

## 【 0 0 1 9 】

サービス提供装置 2 には、認証トークン 1 からの通信データ 1 A を受信する通信装置（第 2 の通信装置）2 1、受信した通信データ 1 A に含まれるトークン ID 1 2 B をキーとして予め登録されているパスワード 2 2 A を検索するデータベース（第 1 のデータベース）、受信した通信データ 1 A に含まれるパスワード 1 2 A と検索したパスワード 2 2 A とを照合する照合回路 2 3、この照合回路 2 3 での照合結果 2 3 A をもとにユーザに提供するサービスを決定し、サービスに対する処理を行う処理装置 2 4 が設けられている。

## 【 0 0 2 0 】

ユーザがサービスを受ける前に、サービス提供装置 2 に対して認証トークンの登録をしておく。

まず、ユーザの所持する認証トークン 1 をサービス提供装置 2 へ接続し、本人



照合装置 1 1 で本人照合を行う。これに応じて、その本人照合結果 1 1 A が照合成功を示す場合は、記憶回路 1 2 に記憶されているトークン I D 1 2 B とパスワード 1 2 A とが通信データ 1 A として通信装置 1 3 からサービス提供装置 2 へ送信される。サービス提供装置 2 の通信装置 2 1 では、受信した通信データ 1 A に含まれているパスワード 1 2 A をトークン I D 1 2 B と関連付けてデータベース 2 2 に登録する。

#### 【 0 0 2 1 】

このとき、サービス提供装置 2 では、データベース 2 2 内にトークン I D 1 2 B に対応するパスワード 1 2 A が登録されていない場合に自動的にそのパスワード 1 2 A を登録するようにしてもよく、操作入力部（図示せず）からの所定操作によりサービス提供装置 2 を登録受付状態としておいてもよい。

また、認証トークン 1 側から、これらパスワード 1 2 A やトークン I D 1 2 B とともに、登録要求を示す情報を送信するようにしてもよい。

#### 【 0 0 2 2 】

次に、ユーザがこのサービス提供装置 2 を利用する際には、まずユーザの所持する認証トークン 1 をサービス提供装置 2 へ接続し、本人照合装置 1 1 で本人照合を行う。これに応じて、その本人照合結果 1 1 A が照合成功を示す場合には、登録時と同様にして、記憶回路 1 2 に記憶されているトークン I D 1 2 B とパスワード 1 2 A とが通信データ 1 A として通信装置 1 3 からサービス提供装置 2 へ送信される。

サービス提供装置 2 では、通信装置 2 1 介して受信した通信データ 1 A に含まれているトークン I D 1 2 B をキーとしてデータベース 2 2 から、上記のようにして登録しておいたパスワード 2 2 A を検索し、通信データ 1 A に含まれているパスワード 1 2 A と照合回路 2 3 で照合する。そして、その照合結果 2 3 A が照合成功を示す場合にのみ処理装置 2 4 で所定の処理が行われ、ユーザに対してサービスが提供される。

#### 【 0 0 2 3 】

このように、本実施の形態では、認証トークン 1 での本人照合結果を送信するのではなく、認証トークン 1 での本人照合結果が照合成功を示す場合にのみ、そ

の認証トークン 1 に予め記憶されているパスワードとトークン ID を送信し、サービス提供装置 2 でそのトークン ID に対応して登録されているパスワードを用いて認証トークンからのパスワードを照合し、その照合結果に基づきサービス提供を行うようにしたので、従来のように認証トークンからの照合成功の結果に基づきサービス提供を行うものと比較して、認証トークンを偽造することが困難となり、サービスの不正利用を防ぐことができる。また、認証トークン情報を用いることで利用ユーザを特定することが可能であり、そのユーザに合わせたサービスの提供が可能となる。

## 【 0 0 2 4 】

次に、図 2 を参照して、本発明にかかる第 2 の実施の形態について説明する。図 2 は第 2 の実施の形態にかかる認証システムを示すブロック図である。

本実施の形態は、前述した第 1 の実施の形態と比較して、サービス提供装置 2 のデータベース 2 2 に対して通信ネットワーク 4 を介して登録情報 3 A を送信する登録装置 3 が追加されている点異なる。

この登録装置 3 には、処理装置 3 1 が設けられており、1 つ以上のサービス提供装置 2 のデータベース 2 2 に対し通信ネットワーク 4 を介して登録情報 3 A すなわちトークン ID とパスワードの組を送信でき、データベース 2 2 を更新することが可能である。

## 【 0 0 2 5 】

このように、登録装置 3 を設けることにより、前述した第 1 の実施の形態のように、個々のサービス提供装置 2 に対して行っていた認証トークンの登録処理を、複数のサービス提供装置 2 に対して一元的に行うことが可能となる。例えば、入室管理システムなどの認証システムでは、サービス提供装置 2 を建物のドアや各部屋のドアなどに複数配置して入室管理する。したがって、本実施の形態を適用すれば、登録装置 3 で複数のサービス提供装置 2 に対して、個々のユーザの認証トークンを容易に登録することができ、認証トークンの登録処理に要する作業負担を大幅に軽減することができる。

## 【 0 0 2 6 】

次に、図 3 を参照して、本発明にかかる第 3 の実施の形態について説明する。

図 3 は第 3 の実施の形態にかかる認証システムを示すブロック図である。

本実施の形態は、前述した第 1 の実施の形態と比較して、サービス提供装置 2 にパスワード発生回路 2 5 を追加し、このパスワード発生回路 2 5 からの新規パスワード 2 5 A により認証トークン 1 のパスワードを更新するようにした点が異なる。

本システムでは、第 1 の実施の形態と同様に、サービス利用前にサービス提供装置 2 に対して認証トークン 1 の登録が行われるとともに、サービス利用時には、本人照合の照合成功に応じて、トークン ID 1 2 B とパスワード 1 2 A とが通信データ 1 A としてサービス提供装置 2 送信され、サービス提供装置 2 で適正なパスワードであることが確認された場合にはサービス提供装置 2 からサービスが提供される。

【 0 0 2 7 】

そして、サービス提供装置 2 の照合回路 2 3 でパスワードの照合が行われ、その照合結果が照合成功を示す場合、パスワード発生回路 2 5 では、新規パスワード 2 5 A を生成し、通信装置 2 1 から認証トークン 1 へ送信するとともに、データベース 2 2 に記憶されているパスワード 2 2 A についても同時に更新する。

認証トークン 1 では、この新規パスワード 2 5 A を通信装置 1 3 で受信し、記憶回路 1 2 内のパスワード 1 2 A を更新する。

【 0 0 2 8 】

このように、サービス提供装置 2 にパスワード発生回路 2 5 を設けて、パスワード照合が成功した後、認証トークン 1 のパスワードを新規パスワードで更新するようにしたので、ユーザがサービスを受けるたびに認証トークン 1 内のパスワードが更新される。

これにより、パスワードが第三者に漏洩した場合でも、次回の利用でのパスワードが更新されるため、認証トークンの偽造がより困難となり、安全なシステムの実現が可能となる。

【 0 0 2 9 】

次に、図 4 を参照して、本発明にかかる第 4 の実施の形態について説明する。

図 4 は第 4 の実施の形態にかかる認証システムを示すブロック図である。

本実施の形態は、前述した第 1 の実施の形態と比較して、認証トークン 1 にパスワードを記憶するデータベース（第 2 の通信装置）14 を追加し、サービス提供装置 2 の装置 ID と対応させてパスワードを管理するようにした点異なる。

本システムでは、第 1 の実施の形態と同様に、サービス利用前にサービス提供装置 2 に対して認証トークン 1 の登録を行うが、この登録時に任意のパスワード、例えばデータベース 14 に予め登録されている初期用のパスワード 14 A を用いる。そしてサービス提供装置 2 では、トークン ID 12 B とそのパスワード 14 A を組としてデータベース 22 へ登録するとともに、記憶回路 26 に予め記憶されている装置 ID 26 A を認証トークン 1 へ送信する。認証トークン 1 では、サービス提供装置 2 からの装置 ID 26 A とパスワード 14 A を組としてデータベース 14 へ登録する。

#### 【0030】

サービス利用時には、認証トークン 1 をサービス提供装置 2 に接続したあと、サービス提供装置 2 から認証トークン 1 へ装置 ID 26 A が送信される。

認証トークン 1 では、本人照合装置 11 でユーザ照合を行い、その本人照合結果 11 A が照合成功を示す場合、通信装置 13 で受信したサービス提供装置 2 からの装置 ID 26 A をキーとしてデータベース 14 からパスワード 14 A を検索する。そして、このパスワード 14 A と認証トークン 12 B とが通信データ 1 A としてサービス提供装置 2 へ送信され、前述と同様に、サービス提供装置 2 で適正なパスワードであることが確認された場合にはサービス提供装置 2 からサービスが提供される。

#### 【0031】

このように、認証トークン 1 にデータベース 14 を設けて、サービス提供装置 2 の装置 ID ごとにパスワードを管理するようにしたので、認証トークン 1 から送信するパスワードを各サービス提供装置ごとに個別に設定でき、各サービス提供装置で複数のパスワードを使い分けることが可能となる。

これにより、1 つのパスワードが漏洩しても、そのパスワードを用いたサービス以外のサービスが不正に利用されてしまうことを防ぐことができるため、認証トークンの偽造がより困難となり、さらに安全なシステムを実現できる。

## 【 0 0 3 2 】

次に、図 5 を参照して、本発明にかかる第 5 の実施の形態について説明する。

図 5 は第 5 の実施の形態にかかる認証システムを示すブロック図である。

本実施の形態は、前述した第 3 の実施の形態に第 4 の実施の形態を適用したものであり、本実施の形態は、前述した第 1 の実施の形態と比較して、サービス提供装置 2 にパスワード発生回路 2 5 が追加されているとともに、認証トークン 1 にパスワードを記憶するデータベース 1 4 が追加されている点が異なる。

処理順序としては、第 4 の実施の形態で説明したように、まず認証トークン 1 のパスワード 1 4 A とトークン I D 1 2 B とをサービス提供装置 2 のデータベース 2 2 へ登録した後、サービス提供装置 2 からの装置 I D 2 6 A とパスワード 1 4 A とを関連付けてデータベース 1 4 へ格納する。

## 【 0 0 3 3 】

サービス利用時、認証トークン 1 では、サービス提供装置 2 へ接続した後、本人照合装置 1 1 でユーザ照合を行い、その成功に応じてサービス提供装置 2 からの装置 I D 2 6 A をキーとしてデータベース 1 4 からパスワード 1 4 A を検索し、そのパスワード 1 4 A とトークン I D 1 2 B とを通信データ 1 A としてサービス提供装置 2 へ送信する。

そして、サービス提供装置 2 の照合回路 2 3 における照合成功に応じて、サービスが提供されるとともに、パスワード発生回路 2 5 からの新規パスワード 2 5 A が認証トークン 1 へ送信され、認証トークン 1 でその新規パスワード 2 5 A と装置 I D 2 6 A とが関連付けられてデータベース 1 4 へ格納される。

## 【 0 0 3 4 】

このように、認証トークン 1 でサービス提供装置 2 の装置 I D に関連付けてパスワードを管理するようにしたので、第 4 の実施の形態と同様に、サービス提供装置毎に異なったパスワードを設定することが可能である。また、ユーザがサービスを受けるごとにパスワードを更新するようにしたので、第 3 の実施の形態と同様に、サービスごとに常に新しいパスワードを設定することが可能となり、パスワードが漏洩しても、サービスが不正に利用されてしまうことを防ぐことが可能となり、認証トークンの偽造がより困難となり、より安全なシステムの実現が可

能となる。

【 0 0 3 5 】

以上で説明した各実施の形態におけるサービス提供装置 2 や認証トークン 1 については、それぞれコンピュータを用いて構成してもよい。その場合、サービス提供装置 2 や認証トークン 1 の各装置や回路部については、それぞれのハードウェア資源とそのハードウェア資源を制御するマイクロプロセッサで実行させるプログラム（ソフトウェア資源）とを協働させることによりそれぞれの機能が実現される。このプログラムについては、ROM、ハードディスクあるいはCD-ROMなどの記録媒体に予め記録しておき、必要に応じてマイクロプロセッサへ読み込んで実行するようにしてもよい。

【 0 0 3 6 】

【発明の効果】

以上説明したように、本発明は、通常時はユーザにより所持されるとともに、ユーザがサービス提供装置を利用する場合はそのサービス提供装置へ接続されてユーザの生体情報に基づきユーザ認証を行う認証トークンを設け、この認証トークンで、当該認証トークンのパスワードと当該認証トークンを識別するためのトークン識別情報とを予め記憶し、ユーザから検出した生体情報をもとにユーザ本人であることを照合し、その照合結果が照合成功を示す場合にパスワードおよびトークン識別情報を通信データとしてサービス提供装置へ送信し、サービス提供装置で、認証トークンのトークン識別情報とパスワードとを第 1 のデータベースで関連付けて予め記憶し、認証トークンから受信した通信データに含まれるパスワードとトークン識別情報をキーとして第 1 のデータベースから検索したパスワードとを照合し、その照合結果に基づきユーザに対してサービスを提供するようにしたものである。

【 0 0 3 7 】

したがって、従来のように認証トークンからの照合成功の結果に基づきサービス提供を行うものと比較して、認証トークンを偽造することが困難となり、サービスの不正利用を防ぐことができる。また、認証トークン情報を用いることで利用ユーザを特定することが可能であり、そのユーザに合わせたサービスの提供が

可能となる。

【図面の簡単な説明】

【図 1】 第 1 の実施の形態にかかる認証システムを示すブロック図である

。

【図 2】 第 2 の実施の形態にかかる認証システムを示すブロック図である

。

【図 3】 第 3 の実施の形態にかかる認証システムを示すブロック図である

。

【図 4】 第 4 の実施の形態にかかる認証システムを示すブロック図である

。

【図 5】 第 5 の実施の形態にかかる認証システムを示すブロック図である

。

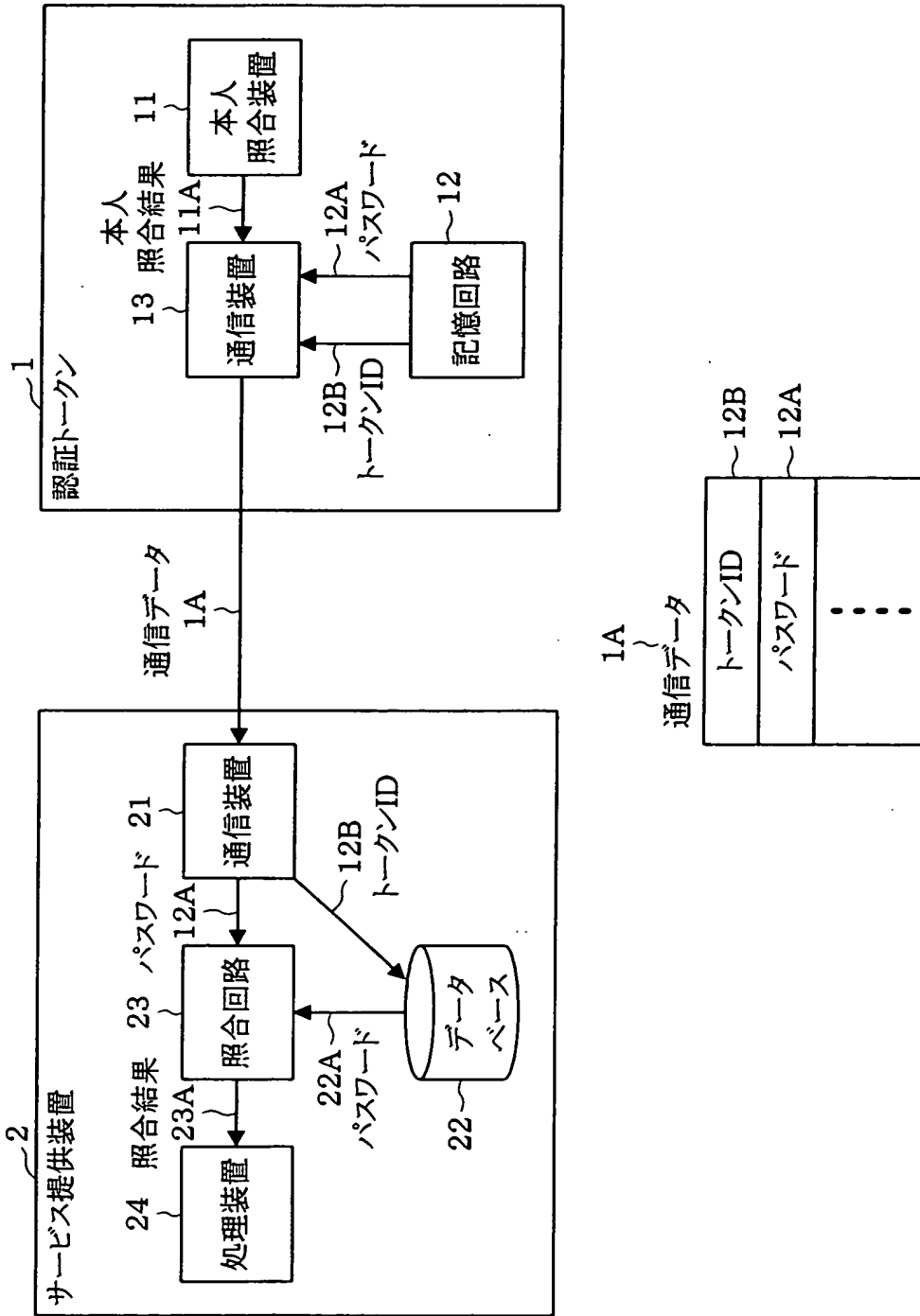
【図 6】 認証システム例を示すブロック図である。

【符号の説明】

1…認証トークン、11…本人照合装置、11A…本人照合結果、12…記憶回路、12A…パスワード、12B…トークンID、13…通信装置、14…データベース、14A…パスワード、1A…通信データ、2…サービス提供装置、21…通信装置、22…データベース、22A…パスワード、23…照合回路、23A…照合結果、24…処理装置、25…パスワード発生回路、25A…新規パスワード、26…記憶回路、26A…装置ID、3…登録装置、31…処理装置、3A…登録情報、4…通信ネットワーク。

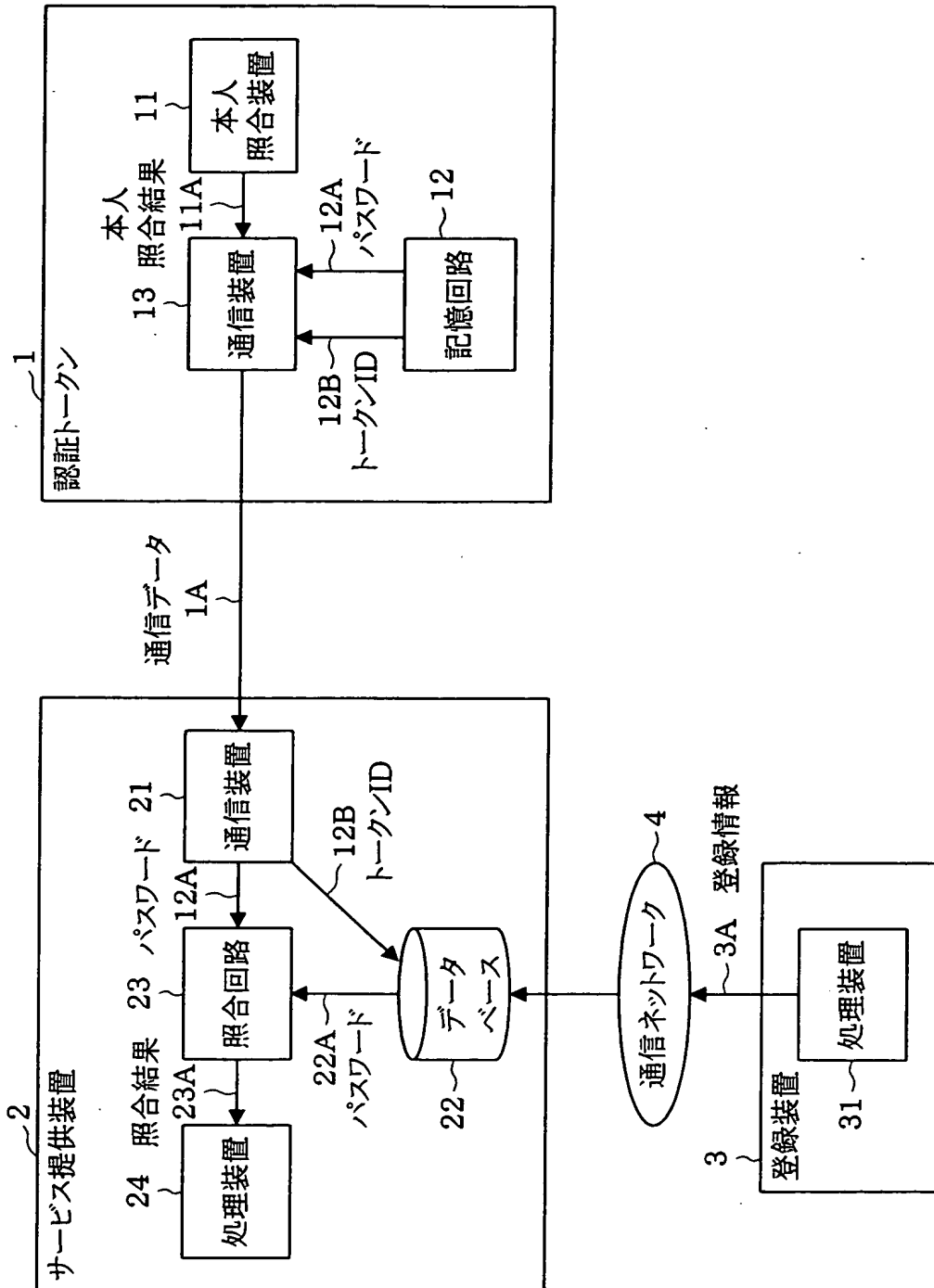
【書類名】 図面

【図 1】

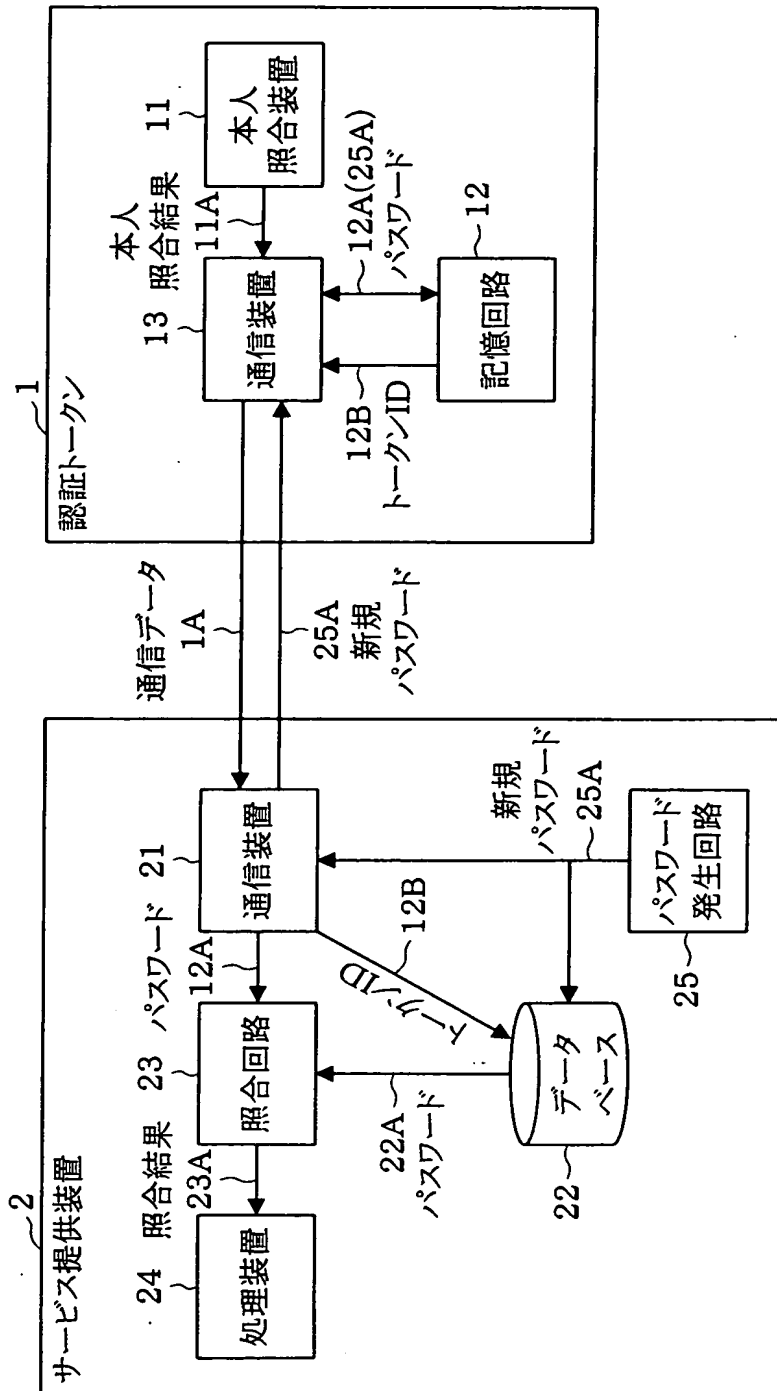




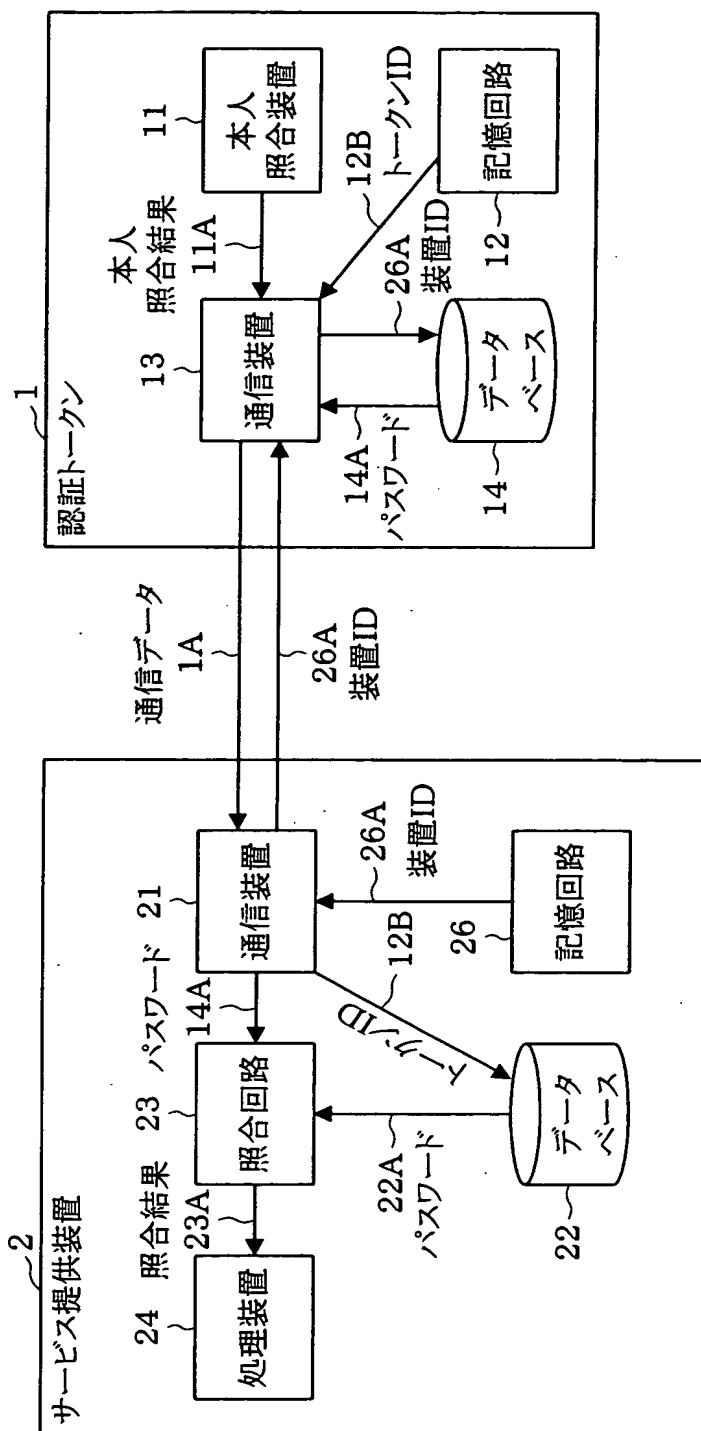
【図 2】



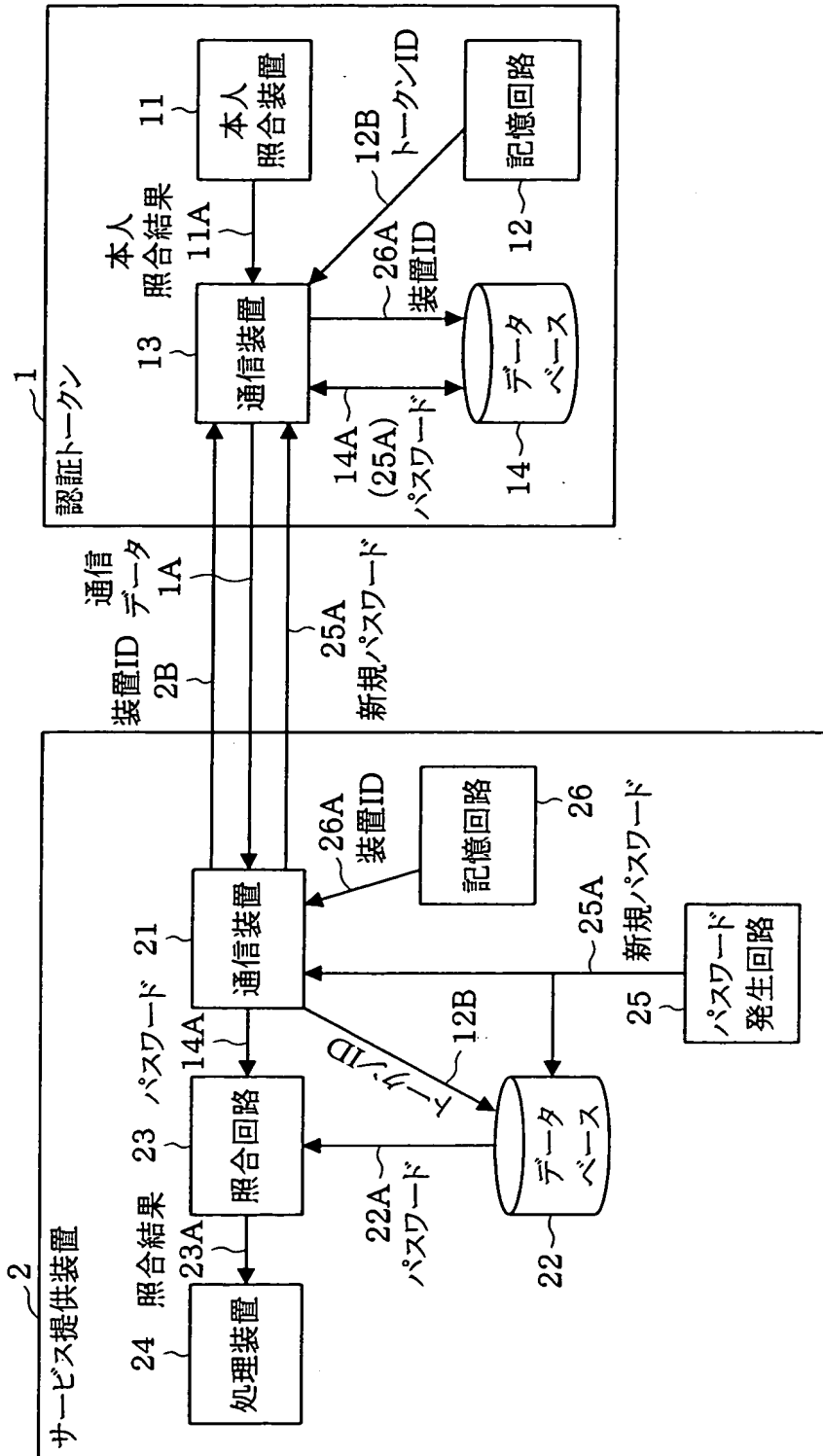
【図 3】



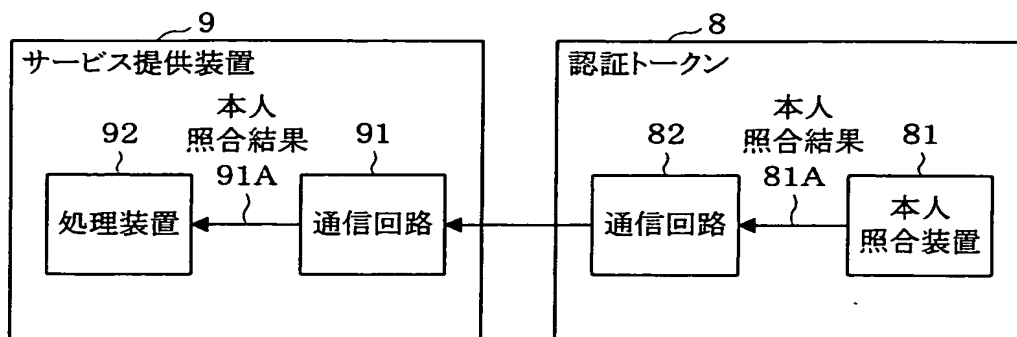
【図 4】



【図 5】



【図 6】



【書類名】            要約書

【要約】

【課題】    サービスの不正利用を防止できるとともに、利用ユーザを特定できるようにする。

【解決手段】    認証トークン 1 の本人照合装置 1 1 による本人照合の結果が照合成功を示す場合にのみ、その認証トークン 1 の記憶回路 1 2 に予め記憶されているパスワード 1 2 A とトークン I D 1 2 B を送信し、サービス提供装置 2 でそのトークン I D 1 2 B に対応してデータベース 2 2 に登録されているパスワード 2 2 A を用いて認証トークン 1 からのパスワード 1 2 A を照合し、その照合結果 2 3 A に基づきサービス提供を行う。

【選択図】            図 1

出 願 人 履 歴 情 報

識別番号 [ 0 0 0 0 0 4 2 2 6 ]

|          |                       |
|----------|-----------------------|
| 1. 変更年月日 | 1 9 9 9 年 7 月 1 5 日   |
| [変更理由]   | 住所変更                  |
| 住 所      | 東京都千代田区大手町二丁目 3 番 1 号 |
| 氏 名      | 日本電信電話株式会社            |